MULTIPLIER AND CIPHER CIRCUIT

Abstract of the Disclosure

A multiplier circuit is disclosed including a Wallace tree block and a carry propagation adder. The Wallace tree block includes a sum calculation block adding partial products for each digit and a carry calculation block adding carries obtained in the addition by the sum calculation block. In the case of multiplication over an extension field (finite field $GF(2^n)$) of two, a result of calculation by the sum calculation block is outputted. The carry propagation adder adds the result of calculation by the sum calculation block and a result of calculation by the carry calculation block. In the case of multiplication for integers (finite field GF(p)), a result of calculation by the carry propagation adder is outputted.